图书情报工作
第62卷 第23期 2018年12月

学术信息资源云存储安全保障架构及防控措施研究*

仇蓉蓉 胡昌平 冯亚飞
武汉大学信息管理学院 武汉 430072

摘要：[目的/意义]信息安全是学术信息资源云存储的重要影响因素，有效的信息安全保障架构和防控措施可以为云存储服务商改进其存储服务提供建议，也可以为用户选择云存储服务平台提供参考。[方法/过程]在对学术信息资源云存储进行安全需求分析的基础上，构建学术信息资源云存储安全部署架构和安全运行架构，并从应用安全保障、内容安全保障、数据安全保障、虚拟化安全保障、基础设施安全保障5个方面对学术信息资源云存储安全防控措施进行研究。其中，应用安全保障包括用户身份认证、用户身份管理、访问控制、应用程序和接口安全4个方面；内容安全保障包括内容安全检测、内容安全控制2个方面；数据安全保障包括数据加密、数据完整性验证、数据确定性删除、数据容灾备份与恢复、数据迁移5个方面；虚拟化安全保障包括安全域隔离、用户数据隔离、多租户管理3个方面；基础设施安全保障包括云存储设施安全、物理环境安全、网络安全3个方面。[结果/结论]安全部署架构为学术信息资源云存储的安全部署提供参考，安全运行架构揭示学术信息资源云存储的安全保障要素和安全保障流程，安全防控措施为学术信息资源云存储提供安全保障技术策略。

关键词：学术信息资源 云存储 安全保障架构 安全防控措施
分类号：G251
DOI：10.13266/j.issn.0252-3116.2018.23.013

1 引言

大数据时代，数据形式的多元化、数据结构的复杂化、增长速度的高速化，导致数字信息资源存储空间需求不断增大、存储形式复杂度不断提高。云存储以其价格低廉、使用便捷、便于管理、高扩展性、弹性配置等特点[1]为不断增长的海量数字信息资源提供了新的存储方式，同时云存储在企业界的广泛应用，也为其快速发展与应用提供了应用平台与实践空间。就学术信息资源而言，云存储的出现为其长期保存提供了新的存储模式，很好地满足了学术信息资源不断发展的数字保存需求。然而，近年来随着Google、Amazon、Apple等云存储服务安全事故频频发生，信息安全问题制约了云存储在业内的快速发展，学术信息资源作为数字信息资源的重要组成部分，其云存储过程中也面临着信息安全问题的困扰。

通过对传统IT模式下学术信息资源存储和学术信息资源云存储的安全需求对比分析，可以看出相比学术信息资源在传统IT模式下的存储，如何将分散的异构学术信息存储资源进行安全整合利用、如何确保学术信息资源云存储的应用安全、如何确保学术信息资源的数据安全等是学术信息资源云存储亟需解决的重要安全问题。具体而言，传统IT模式下学术信息资源被存放在一个物理边界清晰、固定且相对独立的存储环境中，而在云计算环境下由于存储资源的弹性配置、按需分配的特征，云存储安全边界动态变化，无法进行有效划分，学术信息资源管理系统不再具有明确的物理界限，也没有其专属的物理存储设备。因此学术信息资源只能被存放在一个具有逻辑边界的信息管理系统中，如何将地理上分散的学术信息资源进行整合，以形成逻辑上相对独立的存储区域，是学术信息资源云存储面临的重要安全问题之一，目前主要通过虚拟化技术解决；由于学术信息资源云存储不是传统意义上的数据存储，而是一种服务，用户需通过网络访问云端存储资源，因此如何为用户提供一个安全的访问接口、防止非授权用户访问云端学术信息资源等是学

* 本文系国家社会科学重大基金项目"云环境下国家数字学术资源信息安全保障体系研究"（项目编号：14ZDB168）研究成果之一。
作者简介：仇蓉蓉（ORCID：0000-0002-4348-4696），博士研究生，E-mail：zsjj.good@163.com；胡昌平（ORCID：0000-0002-9491-2160），教授，博士生导师；冯亚飞（ORCID：0000-0002-4148-1598），硕士研究生。
收稿日期：2018-05-16 修回日期：2018-08-21 本文起止页码：106-112 本文责任编辑：徐健

术信息资源云存储安全保障的重要方面。传统 IT 环境中用户数据由数据拥有者将其存储在机构、单位的存储设施或个人终端设备上，由数据拥有者或专业人员进行管理。而在云存储环境下，学术信息资源被存放在云端，信息资源拥有者失去了对数据的控制权，云服务商成为学术信息资源云存储安全保障的重要成员，并具有获取访问学术信息资源的权限，如果云服务商的安全规范制度存在漏洞或其内部人员存在非法操作行为等，均可能会引起云存储安全问题，因此在云存储环境下学术资源信息安全风险大大增加。同时，相比其他数字信息，学术信息具有专业、精准、创新价值高等特点，这促使学术信息资源的云存储安全保障对信息的准确性、完整性、有用性提出了更高的要求。同时由于学术信息资源来源众多，其中可能包含一些不合规的内容、敏感信息甚至是违反法律法规的信息，可能会严重影响学术信息的质量，因此如何确保学术信息资源内容的专业性、精准性等内容安全问题是学术信息资源云存储安全保障面临的重要挑战。鉴于此，笔者拟构建学术信息资源云存储的安全保障架构，分析学术信息资源云存储的安全部署模式和安全运行架构，且对学术信息资源云存储的安全防控措施进行研究，以有效实现云存储信息安全保障的长效机制。

2 研究现状

国内外均对学术信息资源的存储安全问题进行了大量研究，数字档案管理系统原型 CLOCKSS(Lots of Copies Keep Stuff Safe)、数字信息资源存储系统 DPN、斯坦福大学的 LOCKSS 系统、DuraSpace 推出的 DuraCloud、保存感知存储服务系统 PDS Cloud、数字化档案馆信息系统 DAITSS(Dark Archive In The Sunshine State)均基于分散保存的方式将多重备份的学术信息资源分散存放:CLOCKSS 对不同区域采用不同的保存模式，以确保系统中的数字信息资源的完整性[2];DPN 将数据副本存放到至少两个不同存储结构的异地存储结点上，以防止由于技术、组织或自然灾害等原因导致的灾难性损失[3];LOCKSS 使用 Opinion polls 机制对保存在多个结点的相同数据进行定期比较和监控，以确保海量数字信息资源的可靠存储[4];DuraCloud 将用户数据存放在不同云存储服务商处并确保所有副本保持同步更新，同时还对用户数据内容的健康状况、完整性进行检测，提高了数据的一致性、安全性和可靠性[5];PDS Cloud 通过利用不同云服务商的异构存储平台和计算平台，为用户提供基于 OAIS(Open Archival Information System)的服务，确保数字信息资源在保存需求动态变化和技术动态变化过程中 PDS Cloud 对长期保存数字内容的可理解性[6];弗罗里达图书馆自动化中心实施的 DAITSS 基于异地进行多重备份，并通过安全存储、安全备份、安全更新、安全迁移来确保档案的长期可用性和完整性[7]。V. J. Sosa-Sosa 等[8]提出了一种在私有云/混合云计算环境中实施的基于开源软件的文件存储架构，并对不同复制技术在私有云和混合云两种不同云存储服务中实施时数据的容错性和可用性进行了比较分析。K. Tang[9]提出了一个数字图书馆灾容系统模型，用于保障云数字图书馆数字信息资源的安全性和信息服务的连续性。

国内主要进行相关理论研究，具体如下:刘万国等从协同管理的角度提出了国家政策法规保障下基于管理层、数据层、云服务平台 3 个层面的国家数字学术信息资源安全保障体系构架[10]，从分级保存的角度提出了包括数字学术资源长期保存的环境情况(主要包括数字学术资源的存在情况、长期保存环境的成熟度)、分级标准体系(包括技术标准、格式标准、价值标准、责任标准、其他标准)、基于数字学术资源生命周期的长期保存等级策略(优先保存级及其保存策略、一般保存级及其保存策略、临时保存级及其保存策略、其他保存级及其保存策略)、长期获取服务 4 个方面的数字学术资源分级保存模型[11]。陈臣等[12]在对数字图书馆云存储安全需求进行分析的基础上，提出了包括访问层(为用户获取云图书馆的联合虚拟参考咨询、个人网络硬盘、远程数据备份、特色库等个性化服务提供了一个便捷的交互界面)、应用接口层(根据实际业务类型，开发不同的应用服务接口，实现云图书馆的二次应用程序开发以及对用户身份的认证和权限分配)、基础管理层(进行存储设施管控、数据处理和数据安全保障，分别实现存储设施的协同工作、数据的分发、处理以及数据的加密和灾容备份)和存储层(由存储设施层和对存储设施进行管理的存储设施管理系统构成，该层对分布式存储资源进行整合，采用统一的管理逻辑和接口实现对文件、目录的标准操作并提供存储空间)的数字图书馆 4 层安全云存储架构。李霜双等[13]提出了包括访问层(该层实现数字学术资源云存储服务用户的账号管理、身份认证、用户授权等)、应用接口层(该层实现网络虚拟化，针对不同云服务模式进行网络安全部署，利用可信网络实现学术信息的传输安全)、基础设施层(该层通过设置物理安全边界实现基础设施的物理安全)、虚拟化层(该层通过虚拟化技术实现

多租户环境下软件和数据的共享安全)和数据中心层(该层实现学术信息的数据安全,主要对学术信息进行加密存储,同时提供学术信息被篡改、攻击等风险时的应用措施)学术信息资源云存储5层安全架构。胡昌平等[14]对国内外学术信息资源云存储服务的安全防控措施进行了研究,并从传输(使用行业标准的安全传输协议)、存储(静态数据加密、身份验证、访问控制、定期完整性检验)、退出(避免数据锁定、多副本异地存储)3个环节对云存储中数据的安全防控措施和数字信息资源云存储服务连续性保障的灾容措施进行了分析。徐国兰[15]基于层次密钥生成与分配策略实施的访问控制安全、基于属性的加密算法进行数据加密、基于虚拟化安全技术对云计算环境下存储设施进行物理隔离、逻辑隔离等安全技术研究数字图书馆云存储安全。经冬鋆[16]采用数据分片存储、数据块加密和设置自我修复机制等安全技术确保高校图书馆云存储安全。中国高等教育文献保障系统CALIS(其组织机构包括全国中心、区域中心和成员馆3个层级)基于层级管理、分散存储的思想确保其学术信息资源的安全:成员馆(由各大高校图书馆组成)部署存储设施、网络设施等基础设施并确保其安全,同时进行著录信息、全文数据库、用户信息等学术信息的保存、备份;区域中心汇集各成员馆的著录信息、用户信息,对学术信息进行整合,基于成员馆提供的API接口开发云服务平台,使学术信息安全风险减少的同时又实现了资源的安全共享;全国中心基于区域中心对所有成员馆学术信息进行整合,统一开发并向用户提供学术信息云服务,用户既可以基于CALIS国家中心站门户提供的云服务使用所有成员馆存储的学术信息,也可以基于区域中心站门户提供的云服务使用区域联盟内所有成员馆存储的学术信息。

通过对国外已有应用案例和已有研究成果的分析可以看出,对于云存储架构研究方面,目前学术信息资源存储系统在理论方面主要基于多个云存储服务平台开发适合行业需求的云存储系统,在实践方面主要对学术信息资源云存储安全保障架构进行研究;在云存储安全防控措施方面,数字信息资源云存储主要基于多重备份、异地备份、异构存储平台备份等方式实现安全、有效的存储。但目前学术信息资源云存储安全保障架构及安全防控措施的大多研究不是很系统,由此,笔者通过对已有理论研究和实际案例的分析,拟构建学术信息资源安全保障架构,同时基于该架构提出相应的安全保障措施。

3 学术信息资源云存储安全保障架构

学术信息资源包括学术成果(如数字期刊、学位论文、学术专著、会议论文、报告等)、科研数据等来源可靠的数字形式的信息资源,以及一些网络信息资源等。例如,高校图书馆的学术信息资源不仅包括信息服务商提供的专业数据库,也包括特色学术信息资源库(如武汉大学的博硕士学位论文库、测绘文摘数据库等)、馆藏书目信息、电子图书、教学视频以及学习软件等。鉴于这些学术信息资源的重要性及其信息安全需求等级的不同,对学术信息资源云存储进行安全部署、确保其安全运行是实现学术信息资源云存储安全保障的关键。笔者基于安全等级保护和分层级保护的思想,分别从云部署模式的角度构建学术信息资源云存储安全部署架构,从运行实施角度构建学术信息资源云存储安全运行架构。

3.1 学术信息资源云存储安全部署架构

由于版权问题或科研保密性要求,学术信息资源云存储需要实现不同等级的安全保障需求。按照安全等级,学术信息资源可以概括为安全等级一般、安全等级较高、安全等级很高三个级别,安全等级越高,其云存储的成本就越高,对云存储信息安全保障能力的要求也就越高。事实上,按照部署模式的不同,云存储可以分为公有云存储、混合云存储、私有云存储,其信息安全保障能力依次逐渐提高。因此,针对不同安全等级的学术信息资源,可以将其存放在具有相应安全保障能力的云中。安全等级一般的学术信息资源存放在公有云中,安全等级较高的学术信息资源存放在混合云中,而安全等级很高的学术信息资源则存放在信息安全保障能力相对最高的私有云中。考虑到不同学术信息资源随着时间变化其安全等级也可能会发生变化,可能需要实现公、私云的权限的变更,因此学术信息资源云存储的安全部署也要确保不同类型的云能够基于安全控制管理(如用户身份、权限管理等)、基于SLA的制定等实现其互操作安全,见图1。

3.2 学术信息资源云存储安全运行架构

通过对学术信息资源云存储安全问题的分析,学术信息资源云存储安全保障涉及安全应用、虚拟化管理、基础设施、数据、内容等方面,因此其安全运行层次架构主要由4个层面(用户层、应用层、管理层、存储层)、5个部分(云存储的应用安全、云存储资源的虚拟化安全、云存储基础设施的安全、数据安全、内容安全)构成,学术信息资源云存储安全运行层次架构的要素

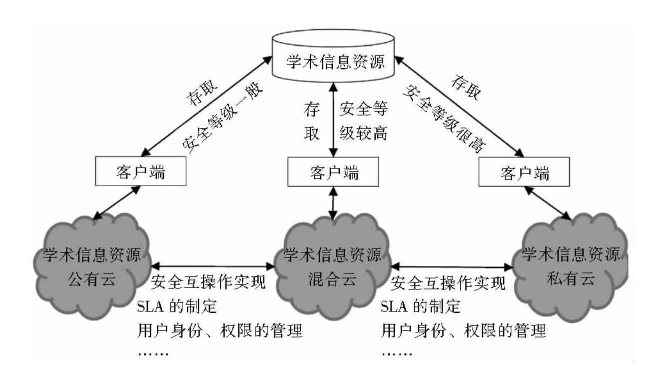


图 1　基于安全等级的学术信息资源云存储部署模式

及其相互间的逻辑关系(见图 2)。其中,应用安全是指在用户与云存储服务的安全交互过程中用户的访问安全和应用程序和接口安全,其安全防控措施包括用户身份认证、用户身份管理、访问控制、应用程序、接口安全;内容安全是指确保存放在云端的数据内容的安全性,包括内容安全检测、内容安全控制;数据安全是指存放在云端的数据的安全,数据安全保障是云存储安全保障的核心和主要目的,主要包括数据加密、数据完整性验证、数据确定性删除、数据容灾备份与恢复、数据迁移;虚拟化安全是指通过虚拟化技术对分散的存储资源实现逻辑上的统一应用过程中存在的安全问题,其安全防控措施包括安全域隔离、用户数据隔离、多租户管理;基础设施安全是指云存储基础设施的安全,包括云存储设施安全、物理环境安全、网络安全,其中云服务商提供的云存储服务其基础设施安全由云服务商保障。

学术信息资源的安全云存储流程主要包括:如何将学术信息资源安全上传至云端、如何确保存储在云端的学术信息资源的安全、学术信息资源云存储服务结束后如何确保数据被安全销毁 3 个环节。具体而言,用户通过客户端登录学术信息资源云存储系统,经过安全访问授权后,用户再通过客户端将学术信息资源上传至学术资源信息系统中,系统通过内容安全模块对学术信息资源进行内容安全分析,内容检测安全后,系统将学术信息资源分解为多个数据包并对数据包分配唯一标识符,同时对其进行加密、备份处理并生成安全迁移版本,系统虚拟化管理模块将数据包分发给在逻辑上实现了安全域隔离、用户数据隔离的分散、异构的云存储设备;学术信息资源被存储在物理设备后,定期验证存储在设备中的数据的完整性,同时确保存储设施安全、物理环境安全、网络安全;结束使用学术信息资源云存储服务时,确保数据被确定性删除以及数据的移植安全。

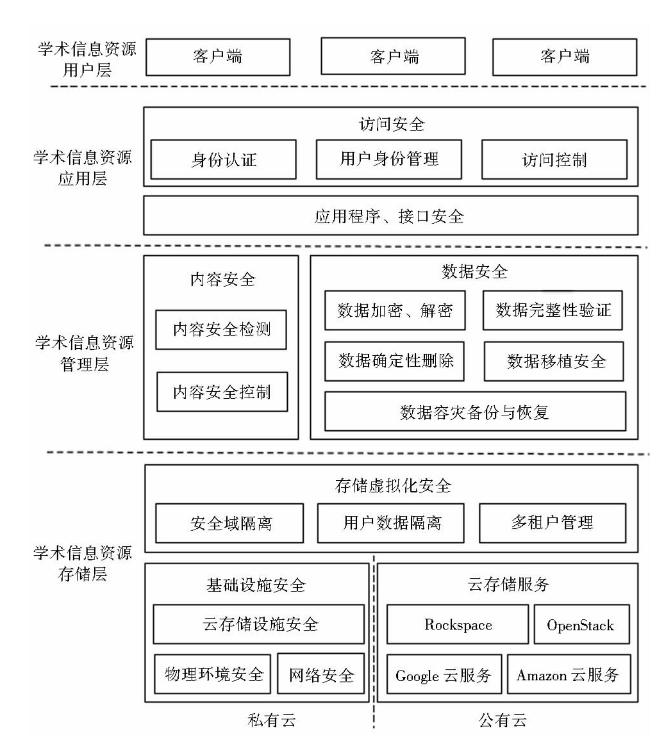


图 2　学术信息资源云存储安全运行层次架构

4　学术信息资源云存储安全防控措施

根据学术信息资源云存储安全需求以及已构建的安全运行架构,本部分将分别从应用安全保障、内容安全保障、数据安全保障、虚拟化安全保障、基础设施安全保障 5 个方面分析其安全防控措施。

4.1　应用安全保障

与传统存储形式相比,云存储是一种将服务外包的存储模式,其在应用过程中需通过远程访问实现,因此云存储应用安全包括用户的访问安全和应用程序、接口安全。传统访问安全主要解决用户在可信存储设备存储数据过程中的安全问题,而在云存储环境下用户和存储设备不在同一个可信域内,内部人员的攻击或服务器被恶意控制都可能造成存储数据的非授权使用[17],其访问安全的保障更复杂。云存储访问安全防控措施主要包括身份认证、用户身份管理和访问控制。身份认证是确认验证主体的真实身份与其声称的身份是否相符,防止非授权用户冒名使用云存储资源。用户身份管理是对云存储用户进行严格的基于角色的用户分类管理,以有效解决云存储用户类型众多、关系复杂的问题。访问控制是为了限制访问主体对访问客体的访问权限,确保用户通过客户端获取存放在云中数据资源时,数据资源不被非授权使用,同时确保应用程序采集的数据资源可以被授权存放在云端。应用程序和接口安全是指云存储的相关软件安全、应用程序的开发、测试安全,相关

API 等接口安全有效,不会因软件、应用程序、接口存在漏洞或被植入木马、病毒造成安全威胁。

4.2 虚拟化安全保障

云存储环境下安全边界动态变化,云存储硬件设施分散、异构,且存在不同用户使用同一台物理设备等交叉使用的情形,因此需要通过虚拟化的方式为学术信息资源云存储系统提供一个安全域以及对用户及其数据进行有效管理,确保逻辑上的存储区域或主体是安全的,其安全保障主要通过安全域隔离、用户数据隔离、多租户管理等安全防控措施来实现。安全域隔离是指通过网络隔离、虚拟防火墙等手段为某类云存储或某个云存储应用营造一个相对稳定、独立的网络环境,防止一个安全域被攻克时影响到其他安全域;用户数据隔离[18-19]主要通过虚拟机隔离实现,由于同一台物理主机上可能有多个用户虚拟机,通过对同一台物理主机上不同用户虚拟机之间、虚拟机与物理机之间的相互隔离,实现对用户数据的隔离,以防止一台虚拟机被攻破时在相同物理主机上的其他用户的虚拟机被越权访问;多租户管理主要解决云存储中基于多租户模式进行有效隔离所产生的安全问题,其通过对虚拟环境租户的登记、分类以及对虚拟资源分配测量的制定,确保不同等级、不同类别租户可以获取相应的虚拟资源权限。

4.3 基础设施安全保障

基础设施安全保障是云存储安全保障的前提,主要为云存储系统的运行提供一个安全可靠的硬件环境,其安全防控措施主要包括云存储设施安全、物理环境安全以及网络安全。存储设施安全是指确保系统运行、人为因素等不会对存储部件、服务器或其他物理计算资源等云存储的硬件存储设施造成破坏;物理环境安全是指云存储设施所处的存储地点和存储敏感信息的安全区域的安全、可靠,一方面存储地能够抵抗地震、水灾、火灾等自然灾害,确保自然灾害不会造成软件、硬件及数据的破坏,另一方面实施物理安全边界并禁止未授权人员访问存储地点;网络安全确保网络传输安全问题,主要是指云存储系统所处网络环境的交换机、路由器、数据包层面的安全。

4.4 数据安全保障

云存储模式造成数据所有权和管理权相分离,导致学术信息资源泄露、学术信息资源丢失等安全风险增加,如云服务商可以获取、搜索存储在云端的学术信息资源,其他攻击者可能通过攻击云服务商获取用户数据[20]。为确保存储在云端的学术信息资源的安全,数据加密、数据完整性验证、数据确定性删除、数据容灾备份与恢复、数字移植安全等是实现学术信息资源云存储安全保障的重要措施。数据加密是指在云存储过程中采用对称加密与非对称加密方式对学术信息资源进行加密,根据不同的加密算法、不同的密钥会生成不同的密文,在密钥未知的情况下无法获取可以被理解的明文信息,从而防止数据被窃取或泄露后其明文数据被获取[21]。数据完整性验证是指检测学术信息资源在传输或存储过程中是否被破坏,数据完整性验证是确保学术信息资源云存储安全的重要措施;数据确定性删除是指学术信息资源被资源拥有者确认删除后,保存在云存储设施中的学术信息资源应确保被彻底删除。数据容灾备份与恢复是指对学术信息资源进行异地备份并按时更新,保证学术信息资源被破坏后可以通过备份数据进行有效恢复[20-22]。数据移植安全是指学术信息资源可以安全移植且以标准化格式导出,方便再次使用其他云存储服务时的数据导入。

4.5 内容安全保障

由于学术信息资的来源众多,加之云存储环境复杂,信息与其发布载体动态绑定使服务器物理位置难以确定,不良信息无法溯源,超大规模数据流量使得在线内容审查十分困难。而学术信息专业性、精准性要求很高,需确保学术信息资源的内容安全,使用户获取准确、有效的知识信息,因此需要对学术信息资源的内容安全进行检测、控制及标准化,其安全防控措施主要包括内容的安全性检测和对有害学术信息资源的内容控制。内容安全性检测是指对学术信息资源中不合规内容(如涉及政治性、健康性、保密性、隐私性、产权性、保护性等方面的内容)、敏感信息甚至违法信息等的检测,主要通过对内容的过滤来实现(如基于关键词的内容过滤和基于语意的内容过滤)。内容安全控制主要指防止基于内容的使用、防止基于内容的破坏和防止基于内容的攻击。其中,防止基于内容的使用是对学术信息资源知识产权的保护,可以通过水印技术或禁止用户复制等方式保护涉密或受版权保护的学术信息资源;防止基于内容的破坏主要是防止病毒对内容造成破坏,可以通过查找内容中的恶意病毒代码消除基于内容的破坏[23]。

5 结语

通过对学术信息资源云存储安全需求的分析,笔者构建了学术信息资源云存储安全部署架构和学术信息资源云存储安全运行架构,旨在为学术信息资源云存储提供一个安全可靠的系统模型;对学术信息资源

云存储的应用安全保障、虚拟化安全保障、基础设施安全保障、数据安全保障、内容安全保障5方面的安全防控措施进行了分析。本研究不足之处在于,仅从理论角度提出学术信息资源云存储安全保障架构和防控措施,缺乏实际系统的搭建与具体防控措施的应用研究。

参考文献:

[1] 傅颖勋,罗圣美,舒继武. 安全云存储系统与关键技术综述[J]. 计算机研究与发,2013,50(1):136 - 154.

[2] CLOCKSS[EB/OL]. [2018 - 05 - 01]. https://clockss. org/clocksswiki/files/CLOCKSS_Handout_Chinese. pdf.

[3] DPN Core[EB/OL]. [2018 - 05 - 01]. http://dpn. org/about.

[4] LOCKSS Preservation Principles[EB/OL]. [2018 - 05 - 01]. https://www. lockss. org/about/principles/.

[5] Features [EB/OL]. [2018 - 05 - 01]. http://www. duracloud. org/details/features.

[6] RABINOVICI - COHEN S, MARBERG J, NAGIN K, et al. PDS cloud: long term digital preservation in the cloud[C]// CAMPBELL R, LEI H, MARKL V. Proceedings of the 2013 IEEE international conference on cloud engineering. Redwood City CA: IEEE,2013:38 - 45.

[7] CAPLAN P. Building a Dark Archive in the Sunshine State: a case study[C]// SOC IMAGING SCI & TECHNOL. Archiving 2005 final program and proceedings. Washington DC: Society for Imaging Science and Technology,2005:9 - 13.

[8] SOSA-SOSA V J, HERNANDEZ-RAMIREZ E M. A file storage service on a cloud computing environment for digital libraries[J]. Information technology&libraries,2012,31(4):34 - 45.

[9] TANG K. Research on disaster recovery model of cloud-based digital library[J]. Applied mechanics and materials,2013,336(1):2134 - 2137.

[10] 刘万国,孙波,刘丁,等. 我国自然科学学术成果流失现状及对策——基于2015年度国家自然科学奖初评获奖人学术论文成果的统计分析[J]. 图书情报工作,2016,60(20):20 - 26,35.

[11] 刘万国,周秀霞,黄颖. 数字学术资源的分级保存模型构建研究[J]. 情报资料工作,2018(2):43 - 47.

[12] 马晓亭,陈臣. 数字图书馆云存储应用系统研究与实现[J]. 图书馆理论与实践,2012(5):8 - 13.

[13] 李霜双,胡昌平. 数字学术信息资源云存储安全保障[J]. 数字图书馆论坛,2017(7):8 - 13.

[14] 胡昌平,王丽丽. 国外面向数字学术资源的云存储服务安全研究[J]. 情报理论与实践, 2018,41(3):156 - 160.

[15] 徐国兰. 云存储在数字图书馆应用中的安全与防范研究[J]. 现代情报,2012,32(4):57 - 59.

[16] 经冬鋆. 高校图书馆云存储基础存储层架构安全问题对策[J]. 图书馆学研究,2014(1):38 - 41.

[17] 王于丁,杨家海,徐聪,等. 云计算访问控制技术研究综述[J]. 软件学报,2015,26(5):1129 - 1150.

[18] 张玉清,王晓菲,刘雪峰,等. 云计算环境安全综述[J]. 软件学报,2016,27(6):1328 - 1348.

[19] 冯朝胜,秦志光,袁丁. 云数据安全存储技术[J]. 计算机学报,2015,38(1):150 - 163.

[20] 李晖,孙文海,李凤华,等. 公共云存储服务数据安全及隐私保护技术综述[J]. 计算机研究与发展,2014,51(7):1397 - 1409.

[21] 傅颖勋,罗圣美,舒继武. 安全云存储系统与关键技术综述[J]. 计算机研究与发展,2013,50(1):136 - 145.

[22] WEI L F, ZHU H J, CAO Z H, et al. Security and privacy for storage and computation in cloud computing[J]. Information sciences, 2014,258(10): 371 - 386.

[23] 雷万云. 信息安全保卫战:企业信息安全建设策略与实践[M]. 北京:清华大学出版社,2013:164 - 165.

作者贡献说明:

仇蓉蓉:设计研究方案,撰写论文;

胡昌平:指导论文写作,修改论文;

冯亚飞:修改论文。

Research on Security Assurance Framework and Control Measures of Academic Information Resource in Cloud Storage

Qiu Rongrong　Hu Changping　Feng Yafei

School of Information Management, Wuhan University, Wuhan 430072

Abstract: [**Purpose/significance**] Information security is an important factor for cloud storage of academic information resources to store in the cloud. Effective information security assurance framework and control measures can provide recommendations for cloud storage service providers to improve their storage services, and it can also offer references for users to choose cloud storage service platforms. [**Method/process**] Based on the security requirement analysis of academic information resources stored in the cloud, this paper built a security deployment framework and a security operation framework for academic information resources to store in cloud. Then, this paper researched the protection and control measures for academic information resources to store in the cloud from five aspects of application security assurance, virtualization security assurance, and infrastructure security assurance, data security assurance, and content security assurance. Application security assurance includes user identity authentication, user identity management, access control, application program and interface security. Virtualization security assurance includes security domain isolation, user data isolation and multi-tenant manage-

ment. The infrastructure security assurance includes cloud storage facility security, physical environment security and network security. Data security assurance includes data encryption, data integrity verification, data assured deletion, data backup and recovery and data migration. Content security assurance includes content security detection and content security control. [**Result/conclusion**] The security deployment framework can provide a reference for the security deployment of the academic information resource to store in the cloud. The security operation framework reveales the security assurance elements and security process for the academic information resources to storage in the cloud. The security prevention and control measures provide the security technology strategy for academic information resources to store in the cloud.

Keywords: academic information resource cloud storage security assurance framework security control measure